Network Working Group
Request for Comments: 1108
Obsoletes: RFC 1038

S. Kent
BBN Communications
November 1991

U.S. Department of Defense Security Options for the Internet Protocol

Status of this Memo

This RFC specifies an IAB standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This RFC specifies the U.S. Department of Defense Basic Security Option and the top-level description of the Extended Security Option for use with the Internet Protocol. This RFC obsoletes RFC 1038 "Revised IP Security Option", dated January 1988.

1. DoD Security Options Defined

The following two internet protocol options are defined for use on Department of Defense (DoD) common user data networks:

CF	CLASS	#	TYPE	LENGTH	DESCRIPTION
1	0	2	130	var.	DoD Basic Security: Used to carry the classification level and protection authority flags.
1	0	5	133	var.	DoD Extended Security: Used to carry additional security information as required by registered authorities.

CF = Copy on Fragmentation

2. DoD Basic Security Option

This option identifies the U.S. classification level at which the datagram is to be protected and the authorities whose protection rules apply to each datagram.

This option is used by end systems and intermediate systems of an internet to:

a. Transmit from source to destination in a network standard representation the common security labels required by computer security models,

b. Validate the datagram as appropriate for transmission from the source and delivery to the destination,

c. Ensure that the route taken by the datagram is protected to the level required by all protection authorities indicated on the datagram. In order to provide this facility in a general Internet environment, interior and exterior gateway protocols must be augmented to include security label information in support of routing control.

The DoD Basic Security option must be copied on fragmentation. This option appears at most once in a datagram. Some security systems require this to be the first option if more than one option is carried in the IP header, but this is not a generic requirement levied by this specification.

The format of the DoD Basic Security option is as follows:

```
+-------------+-------------+-------------+-------------//-----------+
|  10000010   |  XXXXXXXX   |  SSSSSSSS   |  AAAAAAA[1]    AAAAAAA0 |
|             |             |             |        [0]               |
+-------------+-------------+-------------+-------------//-----------+
  TYPE = 130     LENGTH    CLASSIFICATION         PROTECTION
                                LEVEL              AUTHORITY
                                                     FLAGS
```

FIGURE 1. DoD BASIC SECURITY OPTION FORMAT

2.1. Type

The value 130 identifies this as the DoD Basic Security Option.

2.2. Length

The length of the option is variable. The minimum length of the option is 3 octets, including the Type and Length fields (the Protection Authority field may be absent). A length indication of less than 3 octets should result in error processing as described in Section 2.8.1.

2.3. Classification Level

Field Length: One Octet

This field specifies the (U.S.) classification level at which the datagram must be protected. The information in the datagram must be protected at this level. The field is encoded as shown in Table 1 and the order of values in this table defines the ordering for comparison purposes. The bit string values in this table were chosen to achieve a minimum Hamming distance of four (4) between any two valid values. This specific assignment of classification level names to values has been defined for compatibility with security devices which have already been developed and deployed.

"Reserved" values in the table must be treated as invalid until such time they are assigned to named classification levels in a successor to this document. A datagram containing a value for this field which is either not in this table or which is listed as "reserved" is in error and must be processed according to the "out-of-range" procedures defined in section 2.8.1.

A classification level value from the Basic Security Option in a datagram may be checked for equality against any of the (assigned) values in Table 1 by performing a simple bit string comparison. However, because of the sparseness of the classification level encodings, range checks involving a value from this field must not be performed based solely using arithmetic comparisons (as such comparisons would encompass invalid and or unassigned values within the range). The details of how ordered comparisons are performed for this field within a system is a local matter, subject to the requirements set forth in this paragraph.

Table 1. Classification Level Encodings

Value		Name
00000001	-	(Reserved 4)
00111101	-	Top Secret
01011010	-	Secret
10010110	-	Confidential
01100110	-	(Reserved 3)
11001100	-	(Reserved 2)
10101011	-	Unclassified
11110001	-	(Reserved 1)

2.4. Protection Authority Flags

Field Length: Variable

This field identifies the National Access Programs or Special Access Programs which specify protection rules for transmission and processing of the information contained in the datagram. Note that protection authority flags do NOT represent accreditation authorities, though the semantics are superficially similar. In order to maintain architectural consistency and interoperability throughout DoD common user data networks, users of these networks should submit requirements for additional Protection Authority Flags to DISA DISDB, Washington, D.C. 20305-2000, for review and approval. Such review and approval should be sought prior to design, development or deployment of any system which would make use of additional facilities based on assignment of new protection authority flags. As additional flags are approved and assigned, they will be published, along with the values defined above, in the Assigned Numbers RFC edited by the Internet Assigned Numbers Authority (IANA).

a. Field Length: This field is variable in length. The low-order bit (Bit 7) of each octet is encoded as "0" if it is the final octet in the field or as "1" if there are additional octets. Initially, only one octet is required for this field (because there are fewer than seven authorities defined), thus the final bit of the first octet is encoded as "0". However, minimally compliant implementations must be capable of processing a protection authority field consisting of at least 2 octets (representing up to 14 protection authorities). Implementations existing prior to the issuance of this RFC, and which process fewer protection authority than specified here, will be considered minimally compliant so long as such implementations process the flags in accordance with the RFC. This field must be a minimally encoded representation, i.e., no trailing all-zero octets should be emitted. If the length of this field as indicated by this extensible encoding is not consistent with the length field for the option, the datagram is in error and the procedure described in Section 2.8.1 must be followed. (Figure 2 illustrates the relative significance of the bits within an octet).

```
                0   1   2   3   4   5   6   7
              +---+---+---+---+---+---+---+---+
High-order    |   |   |   |   |   |   |   |   |  Low-order
              +---+---+---+---+---+---+---+---+
```

Figure 2. Significance of Bits

b. Source Flags: The first seven bits (Bits 0 through 6) in each octet are flags. Each flag is associated with an authority. Protection Authority flags currently assigned are indicated in Table 2. The bit corresponding to an authority is "1" if the datagram is to be protected in accordance with the rules of that authority. More than one flag may be present in a single instance of this option if the data contained in the datagram should be protected according to rules established by multiple authorities. Table 3 identifies a point of contact for each of the authorities listed in Table 2. No "unassigned" bits in this or other octets in the Protection Authority Field shall be considered valid Protection Authority flags until such time as such bits are assigned and the assignments are published in the Assigned Numbers RFC. Thus a datagram containing flags for unassigned bits in this field for this option is in error and must be processed according to the "out-of-range" procedures defined in section 2.8.1.

Two protection authority flag fields can be compared for equality (=) via simple bit string matching. No relative ordering between two protection authority flag fields is defined. Because these flags represent protection authorities, security models such as Bell-LaPadula do not apply to interpretation of this field. However, the symbol "=<" refers to set inclusion when comparing a protection authority flag field to a set of such fields. Means for effecting these tests within a system are a local matter, subject to the requirements set forth in this paragraph.

Table 2 - Protection Authority Bit Assignments

BIT NUMBER	AUTHORITY
0	GENSER
1	SIOP-ESI
2	SCI
3	NSA
4	DOE
5, 6	Unassigned
7	Field Termination Indicator

Table 3 - Protection Authority Points of Contact

AUTHORITY	POINT OF CONTACT
GENSER	Designated Approving Authority per DOD 5200.28
SIOP-ESI	Department of Defense Organization of the Joint Chiefs of Staff Attn: J6 Washington, DC 20318-6000
SCI	Director of Central Intelligence Attn: Chairman, Information Handling Committee, Intelligence Community Staff Washington, D.C. 20505
NSA	National Security Agency 9800 Savage Road Attn: T03 Ft. Meade, MD 20755-6000
DOE	Department of Energy Attn: DP343.2 Washington, DC 20545

2.5. System Security Configuration Parameters

Use of the Basic Security Option (BSO) by an end or intermediate system requires that the system configuration include the parameters described below. These parameters are critical to secure processing of the BSO, and thus must be protected from unauthorized modification. Note that compliant implementations must allow a minimum of 14 distinct Protection Authority flags (consistent with the Protection Authority field size defined in Section 2.4) to be set independently in any parameter involving Protection Authority flag fields.

a. SYSTEM-LEVEL-MAX: This parameter specifies the highest Classification Level (see Table 1) which may be present in the classification level field of the Basic Security Option in any datagram transmitted or received by the system.

b. SYSTEM-LEVEL-MIN: This parameter specifies the lowest Classification Level (see Table 1) which may be present in the classification level field of the Basic Security Option in any

datagram transmitted by the system.

c. SYSTEM-AUTHORITY-IN: This parameter is a set, each member of which is a Protection Authority flag field. The set enumerates all of the Protection Authority flag fields which may be present in the Protection Authority field of the Basic Security Option in any datagram received by this system. A compliant implementation must be capable of representing at least 256 distinct Protection Authority flag fields (each field must be capable of representing 14 distinct Protection Authority flags) in this set. Each element of the enumerated set may be a combination of multiple protection authority flags.

Set elements representing multiple Protection Authorities are formed by ORing together the flags that represent each authority. Thus, for example, a set element representing datagrams to be protected according to NSA and SCI rules might be represented as "00110000" while an element representing protection mandated by NSA, DOE and SIOP-ESI might be represented as "01011000". (These examples illustrate 8-bit set elements apropos the minimal encodings for currently defined Protection Authority flags. If additional flags are defined beyond the first byte of the Protection Authority Field, longer encodings for set elements may be required.)

It is essential that implementations of the Internet Protocol Basic Security Option provide a convenient and compact way for system security managers to express which combinations of flags are allowed. The details of such an interface are outside the scope of this RFC, however, enumeration of bit patterns is NOT a recommended interface. As an alternative, one might consider a notation of the form COMB(GENSER,NSA,SCI)+COMB(SIOP-ESI,NSA,SCI) in which "COMB" means ANY combination of the flags referenced as parameters of the COMB function are allowed and "+" means "or".

d. SYSTEM-AUTHORITY-OUT: This parameter is a set, each member of which is a Protection Authority flag field. The set enumerates all of the Protection Authority flag fields which may be present in the Protection Authority field of the Basic Security Option in any datagram transmitted by this system. A compliant implementation must be capable of representing at least 256 distinct Protection Authority flag fields in this set. Explicit enumeration of all authorized Protection Authority field flags permits great flexibility, and in particular does not impose set inclusion restrictions on this parameter.

The following configuration parameters are defined for each network port present on the system. The term "port" is used here to refer

either to a physical device interface (which may represent multiple IP addresses) or to a single IP address (which may be served via multiple physical interfaces). In general the former interpretation will apply and is consistent with the Trusted Network Interpretation of the Trusted Computer Systems Evaluation Criteria (TNI) concept of a "communications channel" or "I/O device." However, the latter interpretation also may be valid depending on local system security capabilities. Note that some combinations of port parameter values are appropriate only if the port is "single level," i.e., all data transmitted or received via the port is accurately characterized by exactly one Classification Level and Protection Authority Flag field.

e. PORT-LEVEL-MAX: This parameter specifies the highest Classification Level (see Table 1) which may be present in the classification level field of the Basic Security Option in any datagram transmitted or received by the system via this network port.

f. PORT-LEVEL-MIN: This parameter specifies the lowest Classification Level (see Table 1) which may be present in the classification level field of the Basic Security Option in any datagram transmitted by the system via this network port.

g. PORT-AUTHORITY-IN: This parameter is a set each member of which is a Protection Authority flag field. The set enumerates all of the Protection Authority flag fields which may be present in the Protection Authority field of the Basic Security Option in any datagram received via this port. A compliant implementation must be capable of representing at least 256 distinct Protection Authority flag fields in this set.

h. PORT-AUTHORITY-OUT: This parameter is a set each member of which is a Protection Authority flag field. The set enumerates all of the Protection Authority flag fields which may be present in the Protection Authority field of the Basic Security Option in any datagram transmitted via this port. A compliant implementation must be capable of representing at least 256 distinct Protection Authority flag fields in this set.

i. PORT-AUTHORITY-ERROR: This parameter is a single Protection Authority flag field assigned to transmitted ICMP error messages (see Section 2.8). The PORT-AUTHORITY-ERROR value is selected from the set of values which constitute PORT-AUTHORITY-OUT. Means for selecting the PORT-AUTHORITY-ERROR value within a system are a local matter subject to local security policies.

j. PORT-IMPLICIT-LABEL: This parameter specifies a single Classification Level and a Protection Authority flag field

(which may be null) to be associated with all unlabelled datagrams received via the port. This parameter is meaningful only if PORT-BSO-REQUIRED-RECEIVE = FALSE, otherwise receipt of an unlabelled datagram results in an error response.

k. PORT-BSO-REQUIRED-RECEIVE: This parameter is a boolean which indicates whether all datagrams received via this network port must contain a Basic Security Option.

l. PORT-BSO-REQUIRED-TRANSMIT: This parameter is a boolean which indicates whether all datagrams transmitted via this network port must contain a Basic Security Option. If this parameter is set to FALSE, then PORT-BSO-REQUIRED-RECEIVE should also be set to FALSE (to avoid communication failures resulting from asymmetric labelling constraints).

In every intermediate or end system, the following relationship must hold for these parameters for all network interfaces. The symbol ">=" is interpreted relative to the linear ordering defined for security levels specified in Section 2.3 for the "LEVEL" parameters, and as set inclusion for the "AUTHORITY" parameters.

```
SYSTEM-LEVEL-MAX >= PORT-LEVEL-MAX >=
        PORT-LEVEL-MIN >= SYSTEM-LEVEL-MIN

SYSTEM-AUTHORITY-IN >= PORT-AUTHORITY-IN
                and
SYSTEM-AUTHORITY-OUT >= PORT-AUTHORITY-OUT
```

2.6. Configuration Considerations

Systems which do not maintain separation for different security classification levels of data should have only trivial ranges for the LEVEL parameters, i.e., SYSTEM-LEVEL-MAX = PORT-LEVEL-MAX = PORT-LEVEL-MIN = SYSTEM-LEVEL-MIN.

Systems which do maintain separation for different security classification levels of data may have non-trivial ranges for the LEVEL parameters, e.g., SYSTEM-LEVEL-MAX >= PORT-LEVEL-MAX >= PORT-LEVEL-MIN >= SYSTEM-LEVEL-MIN.

2.7. Processing the Basic Security Option

For systems implementing the Basic Security Option, the parameters PORT-BSO-REQUIRED-TRANSMIT and PORT-BSO-REQUIRED-RECEIVE are used to specify the local security policy with regard to requiring the presence of this option on transmitted and received datagrams, respectively, on a per-port basis. Each datagram transmitted or

received by the system must be processed in accordance with the per-port and system-wide security parameters configured for the system.

Systems which process only Unclassified data may or may not be configured to generate the BSO on transmitted datagrams. Such systems also may or may not require a BSO to be present on received datagrams. However, all systems must be capable of accepting datagrams containing this option, irrespective of whether the option is processed or not.

In general, systems which process classified data must generate this option for transmitted datagrams. The only exception to this rule arises in (dedicated or system high [DoD 5200.28]) networks where traffic may be implicitly labelled rather than requiring each attached system to generate explicit labels. If the local security policy permits receipt of datagrams without the option, each such datagram is presumed to be implicitly labelled based on the port via which the datagram is received. A per-port parameter (PORT-IMPLICIT-LABEL) specifies the label to be associated with such datagrams upon receipt. Note that a datagram transmitted in response to receipt of an implicitly labelled datagram, may, based on local policy, require an explicit Basic Security Option.

2.7.1. Handling Unclassified Datagrams

If an unmarked datagram is received via a network port for which PORT-BSO-REQUIRED = FALSE and PORT-IMPLICIT-LABEL = UNCLASSIFIED (NO FLAGS), the datagram shall be processed as though no Protection Authority Flags were set. Thus there are two distinct, valid representations for Unclassified datagrams to which no Protection Authority rules apply (an unmarked datagram as described here and a datagram containing an explicit BSO with Classification Level set to Unclassified and with no Protection Authority flags set). Note that a datagram also may contain a Basic Security Option in which the Classification Level is Unclassified and one or more Protection Authority Field Flags are set. Such datagrams are explicitly distinct from the equivalence class noted above (datagrams marked Unclassified with no Protection Authority field flags set and datagrams not containing a Basic Security Option).

2.7.2. Input Processing

Upon receipt of any datagram a system compliant with this RFC must perform the following actions. First, if PORT-BSO-REQUIRED-RECEIVE = TRUE for this port, then any received datagram must contain a Basic Security Option and a missing BSO results in an ICMP error response as specified in Section 2.8.1. A received datagram which contains a Basic Security Option must be processed as described below. This

algorithm assumes that the IP header checksum has already been verified and that, in the course of processing IP options, this option has been encountered. The value of the Classification Level field from the option will be designated "DG-LEVEL" and the value of the Protection Authority Flags field will be designated "DG-AUTHORITY."

Step 1. Check that DG-LEVEL is a valid security classification level, i.e., it must be one of the (non-reserved) values from Table 1. If this test fails execute the out-of-range procedure in Section 2.8.1.

Step 2. Check that PORT-LEVEL-MAX >= DG-LEVEL. If this test fails, execute out-of-range procedure specified in Section 2.8.2.

Step 3. Check that DG-AUTHORITY =< PORT-AUTHORITY-IN. If this test fails, execute out-of-range procedure specified in Section 2.8.2.

2.7.3. Output Processing

Any system which implements the Basic Security Option must adhere to a fundamental rule with regard to transmission of datagrams, i.e., no datagram shall be transmitted with a Basic Security Option the value of which is outside of the range for which the system is configured. Thus for every datagram transmitted by a system the following must hold: PORT-LEVEL-MAX >= DG-LEVEL >= PORT-LEVEL-MIN and DG-AUTHORITY =< PORT-AUTHORITY-OUT. It is a local matter as to what procedures are followed by a system which detects at attempt to transmit a datagram for which these relationships do not hold.

If a port is configured to allow both labelled and unlabelled datagrams (PORT-BSO-REQUIRED-TRANSMIT = FALSE) to be transmitted, the question arises as to whether a label should be affixed. In recognition of the lack of widespread implementation or use of this option, especially in unclassified networks, this RFC recommends that the default be transmission of unlabelled datagrams. If the destination requires all datagrams to be labelled on input, then it will respond with an ICMP error message (see Section 2.8.1) and the originator can respond by labelling successive packets transmitted to this destination.

To support this mode of operation, a system which allows transmission of both labelled and unlabelled datagrams must maintain state information (a cache) so that the system can associate the use of labels with specific destinations, e.g., in response to receipt of an ICMP error message as specified in Section 2.8.1. This requirement for maintaining a per-destination cache is very much analogous to

that imposed for processing the IP source route option or for maintaining first hop routing information (RFC 1122). This RFC does not specify which protocol module must maintain the per-destination cache (e.g., IP vs. TCP or UDP) but security engineering constraints may dictate an IP implementation in trusted systems. This RFC also does not specify a cache maintenance algorithm, though use of a timer and activity flag may be appropriate.

2.8. Error Procedures

Datagrams received with errors in the Basic Security Option or which are out of range for the network port via which they are received, should not be delivered to user processes. Local policy will specify whether logging and/or notification of a system security officer is required in response to receipt of such datagrams. The following are the least restrictive actions permitted by this protocol. Individual end or intermediate systems, system administrators, or protection authorities may impose more stringent restrictions on responses and in some instances may not permit any response at all to a datagram which is outside the security range of a host or system.

In all cases, if the error is triggered by receipt of an ICMP, the ICMP is discarded and no response is permitted (consistent with general ICMP processing rules).

2.8.1. Parameter Problem Response

If a datagram is received with no Basic Security Option and the system security configuration parameters require the option on the network port via which the datagram was received, an ICMP Parameter Problem Missing Option (Type = 12, Code = 1) message is transmitted in response. The Pointer field of the ICMP should be set to the value "130" to indicate the type of option missing. A Basic Security Option is included in the response datagram with Clearance Level set to PORT-LEVEL-MIN and Protection Authority Flags set to PORT-AUTHORITY-ERROR.

If a datagram is received in which the Basic Security Option is malformed (e.g., an invalid Classification Level Protection Authority Flag field), an ICMP Parameter Problem (Type = 12, Code = 0) message is transmitted in response. The pointer field is set to the malformed Basic Security Option. The Basic Security Option is included in the response datagram with Clearance Level set to PORT-LEVEL-MIN and Protection Authority Flags set to PORT-AUTHORITY-ERROR.

2.8.2. Out-Of-Range Response

If a datagram is received which is out of range for the network port on which it was received, an ICMP Destination Unreachable Communication Administratively Prohibited (Type = 3, Code = 9 for net or Code = 10 for host) message is transmitted in response. A Basic Security Option is included in the response datagram with Clearance Level set to PORT-LEVEL-MIN and Protection Authority Flags set to PORT-AUTHORITY-ERROR.

2.9. Trusted Intermediary Procedure

Certain devices in an internet may act as intermediaries to validate that communications between two hosts are authorized. This decision is based on the knowledge of the accredited security levels of the hosts and the values in the DoD Basic Security Option. These devices may receive IP datagrams which are in range for the intermediate device, but are not within the accredited range either for the source or for the destination. In the former case, the datagram should be treated as described above for an out-of-range option. In the latter case, an ICMP Destination Unreachable Communication Administratively Prohibited (Type = 3, Code = 9 for net or Code = 10 for host) response should be transmitted. The security range of the network interface on which the reply will be sent determines whether a reply is allowed and at what level it will be sent.

3. DoD Extended Security Option

This option permits additional security labelling information, beyond that present in the Basic Security Option, to be supplied in an IP datagram to meet the needs of registered authorities. Note that information which is not labelling data or which is meaningful only to the end systems (not intermediate systems) is not appropriate for transmission in the IP layer and thus should not be transported using this option. This option must be copied on fragmentation. Unlike the Basic Option, this option may appear multiple times within a datagram, subject to overall IP header size constraints.

This option may be present only in conjunction with the Basic Security Option, thus all systems which support Extended Security Options must also support the Basic Security Option. However, not all systems which support the Basic Security Option need to support Extended Security Options and support for these options may be selective, i.e., a system need not support all Extended Security Options.

The top-level format for this option is as follows:

```
+------------+------------+------------+-------//-------+
|  10000101  |  000LLLLL  |  AAAAAAAA  |  add sec info  |
+------------+------------+------------+-------//-------+
 TYPE = 133      LENGTH     ADDITIONAL      ADDITIONAL
                          SECURITY INFO     SECURITY
                           FORMAT CODE       INFO
```

FIGURE 3. DoD EXTENDED SECURITY OPTION FORMAT

3.1. Type

The value 133 identifies this as the DoD Extended Security Option.

3.2. Length.

The length of the option, which includes the "Type" and "Length" fields, is variable. The minimum length of the option is 3 octets.

3.3. Additional Security Info Format Code

Length: 1 Octet

The value of the Additional Security Info Format Code identifies the syntax and semantics for a specific "Additional Security Information" field. For each Additional Security Info Format Code, an RFC will be published to specify the syntax and to provide an algorithmic description of the processing required to determine whether a datagram carrying a label specified by this Format Code should be accepted or rejected. This specification must be sufficiently detailed to permit vendors to produce interoperable implementations, e.g., it should be comparable to the specification of the Basic Security Option provided in this RFC. However, the specification need not include a mapping from the syntax of the option to human labels if such mapping would cause distribution of the specification to be restricted.

In order to maintain the architectural consistency of DoD common user data networks, and to maximize interoperability, each activity should submit its plans for the definition and use of an Additional Security Info Format Code to DISA DISDB, Washington, D.C. 20305-2000 for review and approval. DISA DISDB will forward plans to the Internet Activities Board for architectural review and, if required, a cleared committee formed by the IAB will be constituted for the review process. Once approved, the Internet Assigned Number authority will assign an Additional Security Info Format Code to the requesting activity, concurrent with publication of the corresponding RFC.

Note: The bit assignments for the Protection Authority flags of the

Basic Security Option have no relationship to the "Additional Security Info Format Code" of this option.

3.4. Additional Security Information.

Length: Variable

The Additional Security Info field contains the additional security labelling information specified by the "Additional Security Info Format Code" of the Extended Security Option. The syntax and processing requirements for this field are specified by the associated RFC as noted above. The minimum length of this field is zero.

3.5. System Security Configuration Parameters

Use of the Extended Security Option requires that the intermediate or end system configuration accurately reflect the security parameters associated with communication via each network port (see Section 2.5 as a guide). Internal representation of the security parameters implementation dependent. The set of parameters required to support processing of the Extended Security Option is a function of the set of Additional Security Info Format Codes supported by the system. The RFC which specifies syntax and processing rules for a registered Additional Security Info Format Code will specify the additional system security parameters required for processing an Extended Security Option relative to that Code.

3.6. Processing Rules

Any datagram containing an Extended Security Option must also contain a Basic Security Option and receipt of a datagram containing the former absent the latter constitutes an error. If the length specified by the Length field is inconsistent with the length specified by the variable length encoding for the Additional Security Info field, the datagram is in error. If the datagram is received in which the Additional Security Info Format Code contains a non-registered value, the datagram is in error. Finally, if the Additional Security Info field contains data inconsistent with the defining RFC for the Additional Security Info Format Code, the datagram is in error. In any of these cases, an ICMP Parameter Problem response should be sent as per Section 2.8.1. Any additional error processing rules will be specified in the defining RFC for this Additional Security Info Format Code.

If the additional security information contained in the Extended Security Option indicates that the datagram is within range according to the security policy of the system, then the datagram should be

accepted for further processing. Otherwise, the datagram should be rejected and the procedure specified in Section 2.8.2 should be followed (with the Extended Security Option values set apropos the Additional Security Info Format Code port security parameters).

As with the Basic Security Option, it will not be possible in a general internet environment for intermediate systems to provide routing control for datagrams based on the labels contained in the Extended Security Option until such time as interior and exterior gateway routing protocols are enhanced to process such labels.

References

[DoD 5200.28] Department of Defense Directive 5200.28, "Security Requirements for Automated Information Systems," 21 March 1988.

Security Considerations

The focus of this RFC is the definition of formats and processing conventions to support security labels for data contained in IP datagrams, thus a variety of security issues must be considered carefully when making use of these options. It is not possible to address all of the security considerations which affect correct implementation and use of these options, however the following paragraph highglights some of these issues.

Correct implementation and operation of the software and hardware which processes these options is essential to their effective use. Means for achieving confidence in such correct implementation and operation are outside of the scope of this RFC. The options themselves incorporate no facilities to ensure the integrity of the security labels in transit (other than the IP checksum mechanism), thus appropriate technology must be employed whenever datagrams containing these options transit "hostile" communication environments. Careful, secure management of the configuration variables associated with each system making use of these options is essential if the options are to provide the intended security functionality.

Author's Address

Stephen Kent
BBN Communications
150 CambridgePark Drive
Cambridge, MA 02140

Phone: (617) 873-3988

Email: kent@bbn.com